Dependability Issues for Intelligent Transmitters and Reliability Pattern Proposal

Florent Brissaud[1,2], Anne Barros[2], Christophe Bérenguer[2], Dominique Charpentier[1]

[1]*Institut National de l'Environnement Industriel et des Risques – INERIS, 60550 Verneuil-en-Halatte, France*
Tel: (33) 3 44 55 69 89; e-mail: florent.brissaud@ineris.fr
[2]*Université de Technologie de Troyes – UTT, 10010 Troyes, France*

Abstract: New technologies make way for "intelligent" transmitters by integrating new functionalities: error measurement corrections, self-adjustment, self-diagnosis for measurement and transmitter status, on-line reconfiguration, and digital bidirectional communication. Industrialists are taking advantage of more accurate measurements, cost reductions and facilities. For industrial risk prevention, new dependability issues are arising. Functionalities such as self-diagnosis and digital communication seem to be in favour of control systems availability. On the other hand, the high amount of electronics and programmable units implies new failure causes and modes which are usually not well known. In this paper, dependability issues for intelligent transmitters are discussed and a reliability model is proposed. By using a *Goal Tree – Success Tree* (GTST) technique, both functional and material aspects of an intelligent transmitter pattern are included. Material-material, material-function, and function-function relationships are then demonstrated in *Master Logic Diagrams* (MLD). These results are proposed as support for further case studies. For example, the impact of any material failure on any function, and the reliability of the main functions, can be assessed using this kind of model. Other dependability tools can take advantage of this reliability pattern, for example when the behavioural aspects of complex systems are undetermined.

Keywords: Intelligent Instrumentation, Dependability, Reliability, Availability, Maintenability, Safety.

1. INTRODUCTION

Sensors and detectors are key parts of safety instrumented systems (SIS). In order to respect the importance of these safety barriers for industrial risk management, dependability issues have to be analysed. The main European standard for the functional safety of SIS is the IEC 61508 (IEC, 2002). It is then necessary to assess the probabilities of failure for each part of the system, including sensors or detectors, in order to define the safety integrity level (SIL).

In the eighties, the development of micro-electromechanical systems (MEMs) led to the revolution of embedded and distributed intelligence systems. The sensors have become "intelligent" and are now able to combine data acquisition, from physical properties, and internal data processing to get the required information. Measurements with detailed results can be transmitted and, for example, certain information about sensor status. These systems are therefore appropriately referred to as "intelligent transmitters" instead of "sensors". Intelligent transmitter definitions and material architecture are presented in Section 2. Moreover, the use of digital technology enables the use of new functionalities which can benefit industrial safety. This is discussed in Section 3. Consequently, new dependability issues arise, especially as regards the possibility of including transmitter functionalities in a reliability model, while taking into account both material and functional interactions. These issues are discussed in Section 4. An example of such a reliability model is then proposed in Section 5. A pattern, which includes basic intelligent transmitter architecture and functionalities, is given as support for further dependability evaluations.

2. WHAT IS AN INTELLIGENT TRANSMITTER?

2.1. Definitions

First, let us suggest a definition of "smart transmitter", less restrictive than "intelligent transmitter": a transmitter is "smart" if some signal conditionings (Smith *et al*., 1995) or data processing (Meijer, 1994) are carried out by an embedded microprocessor, in order to improve metrological performances (CIAME, 2005).

In addition, a transmitter is "intelligent" depending on further functionalities involved in the host system functions: the ability to modify its internal behaviour to optimize data collection and communicate them in a responsive manner (Brignell, 1996); and the bi-directional communication for sending measurement and status information and receiving and processing external commands (IEC, 2006).

This distinction between "smart" and "intelligent" transmitters is, however, not an unbreakable rule (CIAME, 2005). A transmitter is often described as "intelligent" if a microprocessor is embedded for pre-processing tasks (Schodel, 1994) or more advanced functionalities.

2.2. Material architecture

A material architecture, in accordance with IEC 60770-3 (IEC, 2006) and applicable to most of the intelligent transmitters, is presented in Figure 1.

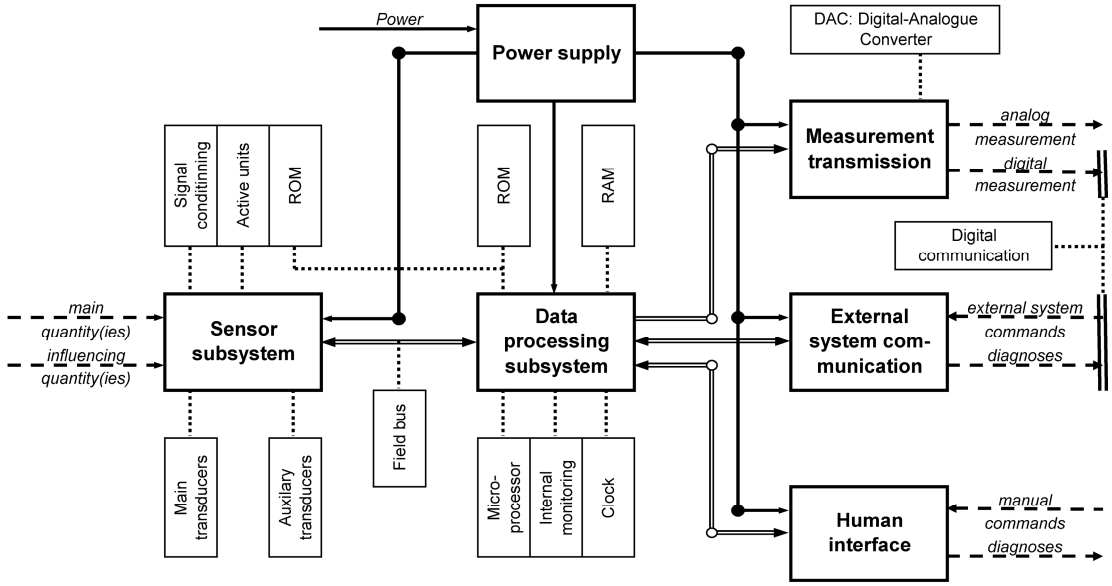

Fig. 1. Intelligent transmitter material architecture

The *sensor subsystem* includes main transducers for converting physical or chemical quantities to be measured (i.e. measurands) into electrical signals, auxiliary transducers for the monitoring of the influencing quantities (temperature, pressure, power supply, dust, etc.), and signal conditioning units. Some active units can be added to execute certain functionalities (see Section 3.1), and memory can be added for the storage of transducer characteristics (ID, metrological parameters, etc.) to be used by the data processing subsystem.

The *data processing subsystem* is the "intelligent" part of the transmitter. It performs data processing (both from sensor and communication subsystems), calculations and functionalities using microprocessors, memory and software. The metrological and functional parameters storage with dates provides some functionality improvements (see Section 3.1).

The communication system is usually composed of several subsystems. The *measurement transmission* may be analogical (with DAC), or digital. In addition, diagnostic information such as measurement characteristics and transmitter status can be transmitted by the subsystem intended for *external system communication*. The 4-20mA medium, proportional to the observed quantity, is the most common in industry. For error diagnoses, an extended signal to 0-24mA can be used (for example, 0mA for a power supply error and 24mA for an out of range error). HART technology (HART, 1999) enables digital communication with a usual 4-20mA medium by a frequency coding. Measurements and diagnoses can therefore both be transmitted in parallel. Power line communication (PLC) can also be used for diagnostic information without additional wires. Field buses (Profibus, Interbus, Device Net, SafetyBus, Modbus, LonWorks, etc.) and wireless networks are also expanding. Standards have been developed to harmonize digital communication, such as OMG, 2003 and IEEE, 2007. Software tools like PACTware (PACTware, 2005) have been designed, field bus independently, for parameters, configuration and diagnostic management with external systems.

3. INTELLIGENT TRANSMITTER TECHNOLOGIES

3.1. Functionalities

New technologies enable the integration of new functionalities in transmitters. Five of them are presented in this section. They play a role in the generic functions, as described by Robert *et al.*, 1993: measure, configure, validate, and communicate. A suggested overall aim is to provide a validated measurement (Robert *et al.*, 1993).

Error measurement correction is one of the most common functionalities. The monitoring of external and internal parameters enables the digital compensation of measurement results in accordance with influencing factors. Storage with the dating of parameters and results can be used to correct linearity and drifts, and to take over missing or absurd measurements. Finally, digital filters may reduce noises.

Self-adjustment is the process through which a transmitter or group of transmitters is run autonomously in order to provide indications corresponding to given values of the measurand. (See IEC 2006 for adjustment, calibration, tuning, and configuring definitions.) Taner *et al.*, 1995 describe four self-adjustment routines which use switches to apply known input signals to the transmitter. Parameters are then set digitally in order that output signals may fit the expected results. Off-set, gain drift, linearity, and temperature adjustments can therefore be done autonomously. If transmitters are redundant, it is possible to make self-adjustments by comparison. In some cases, for example when important drifts are observed through self-diagnosis, adjustments may be ordered by the transmitter itself or by external systems.

Self-diagnosis may use similar procedures as those for self-adjustment to check if expected results are reached when applying appropriate inputs. This can be applied to connections, calculation and data processing units. Internal parameters (temperature of electronics, supply voltage, etc.)

and influencing factors can be monitored to check for acceptable conditions. Mathematical techniques or artificial neural networks can use these data for fault detection and isolation (FDI). (A fault is an abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function (IEC, 2002).) The validation then consists in confirming (or not) the relevance of the transmitted information or, at least, in evaluating a confidence degree. There are different validation levels (Staroswiecki, 2005, CIAME, 2005): technological (for hardware resources), functional (for consistent results), and operational (concerning the control system). Moran *et al.*, 2001 describe three probability estimation algorithms for self-validating transmitters. Finally, an intelligent transmitter is able to transmit information about measurements: qualitative or symbolic quantities, error bounds (Staroswiecki, 2005), confidence in results (Moran *et al.*, 2001); as well as information about the transmitter status (IEC, 2006).

On-line reconfiguration is another functionality which takes advantage of self-diagnoses. Transmitter properties can be modified on-line for metrological requirements (tuning): measuring band and data acquisition frequency according to the observed phenomena and influencing factors. On-line reconfiguration can also have functional purposes: power consumption management and frequency of data transmission. Fault tolerant control (FTC) consists in maintaining transmitter abilities despite abnormal conditions (software errors, faulty components). Transmitter performances may therefore be degraded, but a fault should not develop into a failure at the system level (Blanke *et al.*, 1996). In the event of slight faults, digital compensations can be done (accommodation), similarly to error measurement corrections; otherwise, functional adaptations have to be carried out (restructuring), for example by using redundant material.

Communication between the transmitter and the external systems or the human interface is usually *digital* so that several types of information (measurements, diagnoses) can be transmitted. Moreover, the communication is *bi-directional*: transmitters send measurement and status information, and receive external commands (IEC, 2006).

3.2. Benefits

Intelligent transmitter development seems to be motivated mainly by measurement quality and cost reduction. Error correction and self-adjustment functionalities may improve measurement accuracy by reducing random and systematic errors. Self-diagnoses and on-line configuration can also take part in metrological performances. The direct costs of intelligent transmitters are probably higher due to additional electronics and software used in processing and for functionalities. Nevertheless, these costs are often quite low compared to wiring, installation, and maintenance (CIAME, 1987). From this point of view, intelligent transmitters are appealing to the purchaser, due to their special functionalities. In particular, wiring costs may be reduced by field buses. Finally, digital communication and other functionalities, such as self-adjustment and on-line reconfiguration, make transmitters easier to use and save time (Mintchell, 2001).

3.3. Intelligent transmitters and industrial risk prevention

The main transmitter manufacturers propose intelligent systems for industrial safety. The first were differential pressure transmitters, produced since the 1980's (CIAME, 1987). Nowadays, multivariable transmitters combine differential and static pressure, internal and external temperature, and flow rate measurements. A lot of measurement corrections, advanced self-diagnoses, and some reconfigurations are available. Temperature transmitters, installed in pairs, perform self-diagnoses and on-line reconfigurations when faults or failures occur. Infrared gas or flame detectors can usually make error measurement corrections according to dust accumulation, temperature (a significant influencing factor for gas concentration), climate, ageing, etc. Moreover, self-adjustments and diagnoses are also available quite often. Remote control systems for transmitter adjustment and diagnosis, using networks, have also been developed by some manufacturers.

4. DEPENDABILITY ISSUES

4.1. Benefits for dependability?

Although intelligent transmitter provide practical benefits, it is advisable that the effect of their functionalities on dependability be analysed. In this section, a priori advantages and disadvantages of "intelligence" in transmitters are discussed in terms of reliability, maintainability, and safety.

Reliability refers to an item's ability to perform a required function under given conditions for a given time interval (IEC, 1990). The high amount of electronics, programmable units, and software aspects implies new failure causes and modes which are usually not well known. Software errors in particular are very unpredictable (Garret, 2002) and may affect a lot of transmitted information (measurements, diagnoses). To some extent, these disadvantages can be compensated for by fault tolerant strategies, for example by using on-line reconfiguration. Moreover, some faults or failures which appear with ageing, such as drifts, can be prevented by self-adjustments. On the other hand, these functionalities can themselves be the source of additional failures if they are not run correctly, due to hardware or software faults. Digital communication gives rise to the same dilemma. Although it is suggested that wire reduction improves reliability (Smith *et al.*, 1995), field buses transport a lot of information which implies that they play a vital role in reliability, especially in terms of common cause failures.

Maintainability takes advantage of self-diagnoses and digital communication. This refers to an item's ability to be maintained in or restored to a state within which it is able to perform a required function (IEC, 1990). Information about drifts, influencing factors, charge exceeding, power supply, etc., may be monitored over time, as well as faults and failures with corresponding circumstances. Preventive maintenance can therefore be optimized by using these data, for example, by predicting any failure occurrences. Field buses and on-line reconfiguration make corrective maintenance easier than heavy wires and non-adaptive systems (Mintchell, 2001).

Safety refers to the ability to avoid unacceptable harm to any given operation. Self-diagnoses allow a better fault and failure coverage which improves safety. In the event of failure detection, safe states can also be defined in more detail. Centralized data processing and digital communication may also improve the efficiency of global risk management.

4.2. Intelligent transmitter dependability evaluation

Reliability criteria are often used as input data for self-diagnoses and validation (Moran *et al.*, 2001, Staroswiecki, 2005), on-line reconfiguration (Guenab *et al.*, 2006), and in the design of intelligent transmitter networks (Dai *et al.*, 2003, Bhushan *et al.*, 2008). However, they are seldom subject to evaluation.

The dependability of digital communication, especially using field buses, has been studied in many works. Cauffriez *et al.*, 2004 present field bus constraints regarding dependability, and failure modes and effect analyses (FMEA) are given. Barger *et al.*, 2004 quantify the availability of a control system made up by communication network, sensors, control units, and actuators, with coloured Petri nets. In order to take transmission faults into account in field bus availability assessments, Ghostine *et al.*, 2006 use stochastic activity networks (SANs). In both of these approaches, results are obtained by Monte Carlo simulations. Digital communication is usually assessed regardless of the nature of the transmitter, regarded as a "black box", which can be either operational or not. The "intelligent functions" and the different failure modes are therefore not taken into account.

Meulen, 2004 aims to analyse common cause failure issues for intelligent transmitters. Failure modes and effect analyses have been proposed in this area. New failure causes have been highlighted compared to other transmitters, which can result in new common cause failure modes.

4.3. Dependability issues

Using intelligent transmitters for industrial risk prevention requires dependability evaluations. However, the literature pertaining to these assessments is scarce and seldom includes all the intelligent transmitter particularities. This kind of dependability evaluation should deal with several issues:

i. intelligent transmitters are complex systems, that is, numerous interactions exist between components, and also between functions (e.g. self-adjustment may change parameters which are then used in data processing, on-line reconfiguration can modify transmitter performances, etc.)

ii. the behaviour of certain transmitter components, such as programmable units and software, is difficult to predict when faults or failures occur, and may be heterogeneously shared between several functions

iii. transmitted data are numerous (measurement, diagnoses), sometimes continuous-natured, and can all be required for control system decisions; all information that may potentially fail, including combinations (e.g. good measurement but bad state information, and vice-versa), must therefore be assessed

iv. due to new technologies that are being used, few qualitative (observed failure modes) and quantitative (reliability data) dependability feedback is available.

A qualitative dependability study such as FMEA is therefore hardly exhaustive. Moreover, *ii* and *iii* make binary tools (fault trees, reliability block diagrams) inappropriate as it. Moreover, transition states approaches (Markov analysis, Petri Nets) have some difficulty in defining functional and dysfunctional states because of *i* and *ii*. A reliability pattern, proposed in the next section, will therefore aim to represent all these intelligent transmitter aspects in the same model.

5. RELIABILITY MODEL PROPOSAL

5.1. A model for intelligent transmitters

Two approaches may be distinguished for complex systems modelling: function-oriented (FO) and object-oriented (OO). FO models aim to analyse the system according to goals and functions which are to be met, including interactions. It is used in the design phase for requirements definitions, and in order to understand the effective operation of the system. *Structural Analysis and Design Technique* (SADT), as proposed by Robert *et al.*, 1993 for intelligent transmitters, *Functional Analysis System Technique* (FAST), *Multilevel Flow Modelling* (MFM), and some UML or SysML diagrams as *Use Case Diagram* are examples of these approaches. OO models give the system structural breaking up with material interactions, such as *Fault Tree* and UML *Class Diagram* (denoted *Block Definition Diagram* in SysML), as proposed by Luttenbacher *et al.*, 1995 for intelligent transmitters. Several tools are then available for dependability evaluations using these approaches. Behavioural (or operational) aspects are obtained by linking together functional and material representations. If system behaviour is well-known, safe-SADT (Benard *et al.*, 2008), which has been developed for the design phase, may be used to include this property.

For the present study, the GTST-MLD model, proposed by Modaress *et al.*, 1999 has been chosen. An attractive characteristic of this approach is to give both a functional analysis of the system, using *Goal Tree* (GT), and a material breaking up, using *Success Tree* (ST), in a similar and intuitive manner. Material-material, material-function, and function-function relationships are then included by *Master Logic Diagrams* (MLD), which represent behavioural aspects. This kind of model has already been applied for dependability analyses, for example by Jalashgar, 1998 to identify some complex system failures. A reliability model for an intelligent transmitter pattern is proposed in Figure 2, including basic material architecture detailed in Section 2.2, and functionalities presented in Section 3.1. The *functional tree* (i.e. GT) breaks the system *goal* up into *global* and *basic* (or *physical*) functions. A distinction is made between *main* and *supporting* functions. The latter have no final goal as far as users are concerned, but are required and act on main functions. For example, self-adjustment may define digital parameters which are used for data processing. In the same way, a *material tree* (i.e. ST) is made up of *system*, *subsystem* and *unit* elements, as well as main and supporting materials.

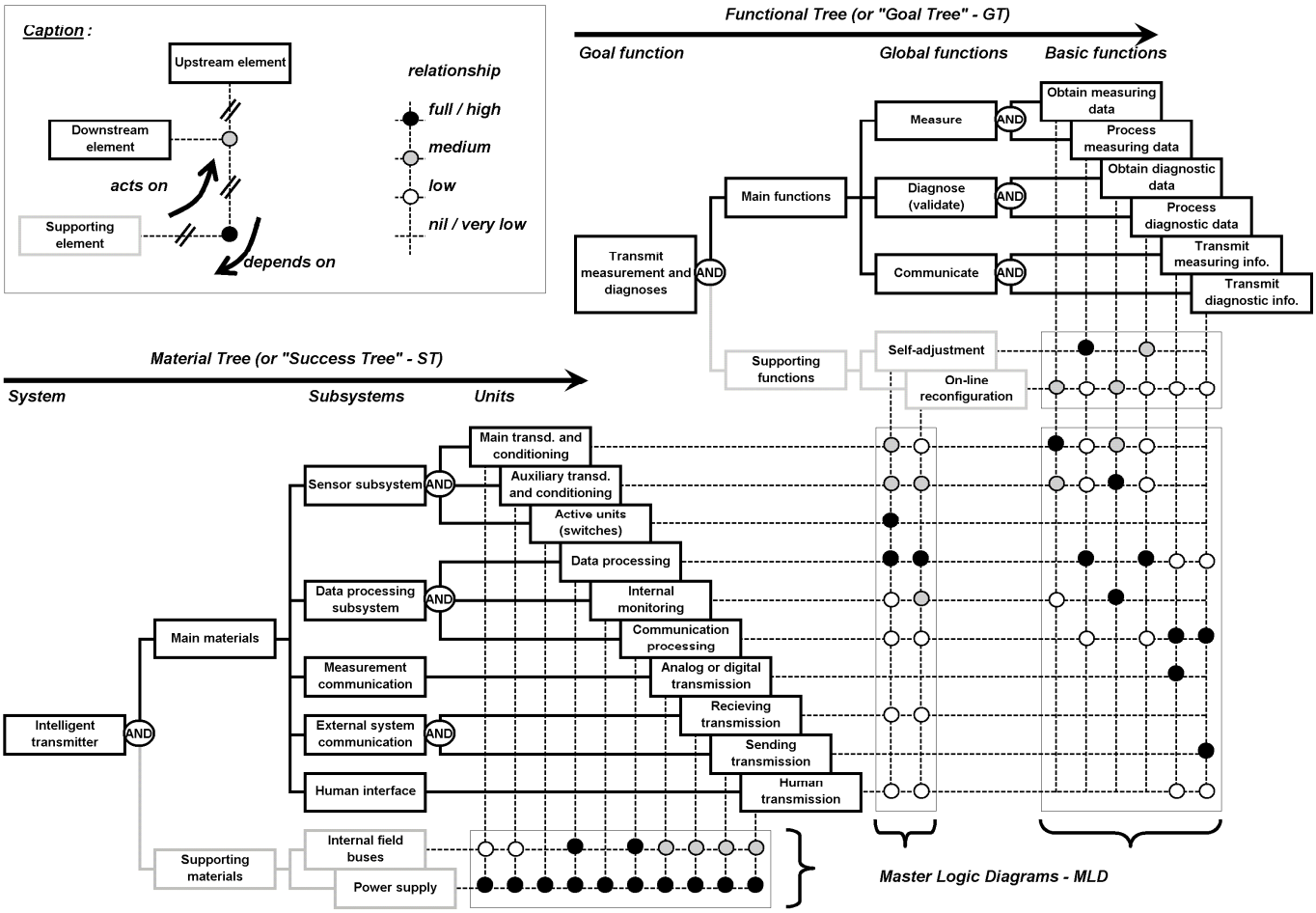

Fig 2. Reliability model proposal for an intelligent transmitter pattern

Finally, MLD consist of circles in colours which represent the relationships between downstream and upstream elements. For example, to obtain diagnostic data, auxiliary transducers are always required (black dots), whereas in some cases, even if these transducers are in failed states, self-adjustment can be satisfactorily performed (grey dots). The impacts of any failures or malfunctions can then be divided among other material and functional performances, according to assumed relationships. This particularity differs from binary approaches and transition state models where states have to be strictly defined. Since Figure 2 is just a pattern, this model has to be adapted to specific case studies.

5.2. Prospects for reliability analyses

From this model, some analyses have been proposed by Brissaud *et al.*, 2008, 2009 by translating MLD components into probabilistic values. With basic reliability formulas, it is then possible to assess the total resulting relationships between any material and any function, taking into account direct and indirect (i.e. via supporting elements) relationships. Including material unreliability functions, the probability of each main function malfunctioning can be assessed, as well as possible combinations (e.g. good measurement but false diagnosis, and vice-versa). Further discussions and prospects for quantitative analyses are given by Hu *et al.*, 1999 and Brissaud *et al.*, 2008, 2009.

6. CONCLUSION

This paper has examined intelligent transmitters. Definitions and basic material architecture are proposed. Several functionalities may be carried out by these systems: error measurement corrections, self-adjustment, self-diagnoses, on-line reconfiguration, and digital bidirectional communication. The benefits for industrialists are numerous and motivate the use of these technologies for risk prevention. The intelligent transmitters' dependability therefore needs to be assessed. Reliability, maintainability and safety aspects are further discussed. Such evaluations are quite seldom in literature and usually do not include "intelligent particularities". In fact, classical dependability tools have to deal with some difficulties due to the system complexity and lack of behavioural knowledge. A reliability model is therefore proposed, using an intelligent transmitter pattern. GTST aims at representing both material and functional aspects, and the relationships between these elements are given in MLD. Basic material architecture and system functionalities are included in the model, in order to be used as support for further case studies. Some analyses can be expected, as the assessment of any material failure impact on any function, and the functions' reliability. Other dependability tools can take advantage of this reliability pattern, for example when system behavioural aspects are not well known.

REFERENCES

Barger, P., Thiriet, J.M., Robert, M. and Aubry, J.F. (2004). Dependability study in distributed control systems integrating smart devices. In: *Cost Oriented Automation 2004*. Ottawa.

Benard, V., Cauffriez, L. and Renaux, D. (2008). The Safe-SADT method for aiding designers to choose and improve dependable architectures for complex automated systems. *Reliability Engineering & System Safety*, 93, 179-196.

Blanke, M., Izadi-Zamanabadi, R., Bogh, S.A. and Lunau, C.P. (1996). Fault-tolerant control systems - A holistic view. *Control Engineering Practice*, 5, 693-702.

Brignell, J. E. (1996). The future of intelligent sensors: A problem of technology or ethics? *Sensors And Actuators A-Physical*, 56, 11-15.

Brissaud, F., Charpentier, D., Barros, A. and Bérenguer, C. (2008). Intelligent Sensors: New Technologies and New Dependability issues. In: *λμ16*. Avignon.

Brissaud, F., Charpentier, D., Barros, A. and Bérenguer, C. (2009). Reliability Study of an Intelligent Transmitter. In: *15th ISSAT International Conference*. San Francisco.

Bhushan, M., Narasimhan, S. and Rengaswamy, R. (2008). Robust sensor network design for fault diagnosis. *Computers & Chemical Engineering*, 32, 1067-1084.

Cauffriez, L., Ciccotelli, J., Conrard, B. and Bayart, M. (2004). Design of intelligent distributed control systems: a dependability point of view. *Reliability Engineering & System Safety*, 84, 19-32.

CIAME (1987). *Livre Blanc, Les capteurs intelligents : Réflexion des utilisateurs*. AFCET, Paris.

CIAME: Bayart, M., Conrard, B., Chovin, A. and Robert, M. (2005). Capteurs et actionneurs intelligents. *Technique de l'Ingénieur*, S 7 520.

Dai, Y.S., Xie, M., Poh, K.L. and Liu, G.Q. (2003). A study of service reliability and availability for distributed systems. *Reliability Engineering & System Safety*, 79, 103-112.

Garrett C.J. and Apostolakis, G.E. (2002). Automated hazard analysis of digital control systems. *Reliability Engineering & System Safety*, 77, 1-17.

Ghostine, R., Thiriet, J.M. and Aubry, J.F. (2006). Dependability evaluation of networked control systems under transmission faults. In: *6th IFAC symposium*. Beijing.

Guenab, F., Theilliol, D., Weber, P., Zhang, Y.M. and Sauter, D. (2006). Fault tolerant control system design: a reconfiguration strategy based on reliability analysis under dynamic behaviour constraints. In: *6th IFAC symposium*. Beijing.

HART (1999). *HART Field communication protocol - Application guide HCF LIT 34*. HART Communication Foundation, Austin.

Hu, Y. and Modarres, M. (1999). Evaluating system behavior through Dynamic Master Logic Diagram (DMLD) modelling. *Reliability Engineering & System Safety*, 64, 241-269.

Institute of Electrical and Electronics Engineers [IEEE] (2007). *1451 Smart Transducer Interface for Sensors and Actuators*. IEEE Standard, New York.

International Electrotechnical Commission [IEC] (1990). *IEC 60050(191) International Electrotechnical Vocabulary, Chapter 191*. IEC Standard, Geneva.

International Electrotechnical Commission [IEC] (2002). *IEC 61508 Functional safety of electrical / electronic / programmable electronic safety-related systems*. IEC Standard, Geneva.

International Electrotechnical Commission [IEC] (2006). *IEC 60770-3 Transmitters for use in industrial-process control systems, Part 3*. IEC Std., Geneva.

Jalashgar, A. (1998). Identification of hidden failures in process control systems based on the HMG method. *International Journal of Intelligent Systems*, 12, 159-179.

Luttenbacher, D., Roth, S., Robert, M. and Humbert, C. (1995). Intelligent Sensor - Object Approach. *Control Engineering Practice*, 3, 805-812.

Meijer, G.C.M. (1994). Concepts and focus point for intelligent sensor systems. *Sensors And Actuators A-Physical*, 41, 183-191.

Meulen, van der M.J.P. (2004). On the use of smart sensors, common cause failure and the need for diversity. In: *6th International Symposium Programmable Electronic Systems*. Cologne.

Mintchell, G. (2001). Use Sensors Intelligently. *Control Engineering*, January.

Modarres, M. and Cheon, S.W. (1999). Function-centered modeling of engineering systems using the goal tree-success tree technique and functional primitives. *Reliability Engineering & System Safety*, 64, 181-200.

Moran, A.W., O'Reilly, P.G. and Irwin, G.W. (2001). Probability estimation algorithms for self-validating sensors. *Control Engineering Practice*, 9, 425-438.

Object Management Group [OMG] (2003). *Smart Transducers Interface Specification*. Object Management Group Inc., Needham.

PACTware (2005). *PACTware Efficient configuration*. PACTware Consortium e.V., Pfinztal.

Robert, M., Marchandiaux, M. and Porte, M. (1993). *Capteurs intelligents et méthodologie d'évaluation*. Hermes, Paris.

Schodel, H. (1994). Utilization of fuzzy techniques in intelligent sensors. *Fuzzy Sets and Systems*, 63, 271-292.

Smith, G. and Bowen, M. (1995). Considerations for the utilization of smart sensors. *Sensors And Actuators A-Physical*, 47, 521-524.

Staroswiecki, M. (2005). Intelligent sensors: A functional view. *IEEE Transactions On Industrial Informatics*, 1, 238-249.

Taner, A.H. and Brignell, J.E. (1995). Aspects of intelligent sensor reconfiguration. *Sensors And Actuators A-Physical*. 47, 525-529.